In the Drawings:

Figure 1 has been amended to include identifying numeral 10 as referred to in the specification on page 5, line 4-5. A replacement sheet for Fig. 1 containing this amendment is attached.

REMARKS

Claims 1-51 are pending in the application and subject to examination. Claims 1, 3, 6, 10, 23, 25, 27, 29, 36, 38, 39 and 43 are amended herein. Claims 46-51 are new.

The Amendments and New Claims

The amendments to independent claim 1 relate to a mobile client being permitted to roam on the network, and the process that ensues when the mobile client is handed off from one access point to another while roaming. In particular, the amendments, reproduced below, specify that the mobile client is associated with the newly located access point and allowed to continue to access the network but only "upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access to the network":

> "when access is granted, permitting roaming of the mobile client within the network;
>
> during said roaming, when signal quality from a current access point in communication with the mobile client deteriorates sufficiently, locating another access point;
>
> when another access point is located, associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network."

The amendments to independent claim 39, reproduced below, are similar:

> "deciding means for deciding whether to grant or deny the ~~user station~~client access to the network based on the authenticity of the identity and the comparison of the location information, and, when access is granted, permitting roaming of the mobile client within the network;
>
> locating means for locating another access point upon detecting, during said roaming, when signal quality from a current access point in communication with the mobile client has deteriorated sufficiently;
>
> second associating means for associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing

updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network."

These amendments to independent claims 1 and 39 are supported, for example, by page 12, line 21, to page 13, line 15.

The amendments to independent claim 10 relate to a data structure, accessible by the authentication server, associating identities of clients with their authorized access locations on the network. In particular, the amendments, reproduced below, specify that the authentication server utilizes this data structure to determine whether to grant or deny the client access to the network based in part of the current location information for the client. The amendments also feature a network manager that allows a network administrator to create and update the data structure:

"a network;

an authenticator for requesting an identity from a client and for associating location information corresponding to the client with the identity; ~~and~~

a data structure, accessible by an authentication server, associating identities of clients with their authorized access locations;

~~an~~the authentication server, upon receiving the identity and associated location information from the authenticator, ~~for~~ deciding whether to grant or deny the client access to the network ~~based on the identity and the location information~~ by accessing the data structure and determining that the location information corresponding to the client specifies a location that is one of the authorized access locations, if any, for the client as maintained in the data structure; and

a network manager that allows a network administrator to create and update the data structure."

The amendments to independent claim 27, reproduced below, are similar, except that they call for the network manager to be directly connected to the authentication server:

"a data structure, accessible by an authentication server, associating identities of clients with their authorized access locations;

~~an~~the authentication server ~~for~~ deciding whether to grant or deny each of the user stations access to the network ~~based on the corresponding identity and location information~~ by accessing the data structure and determining, for each user station, that the location information corresponding to the user station specifies a location that is one of the authorized access locations, if any, for the user station as maintained in the data structure; and

a network manager, directly connected to the authentication server, that allows a network administrator to create and update the data structure."

These amendments to independent claims 10 and 27 are supported, for example, by page 9, lines 1-16, and page 6, lines 11-17.

The amendments to claims 1, 10, 27 and 39 also include removing the last two paragraphs of each, which were added in the Response dated October 30, 2008. While these two paragraphs also relate to roaming, and therefore are similar to the limitations added to independent claims 1 and 39 in this response, a critical difference is that the added limitations relate to the procedure that ensues when the mobile, while roaming, is handed off from one access point to another. As will be seen, this added requirement of a handoff from one access point to another materially distinguishes these added limitations from the two paragraphs because the prior art does not teach and in fact teaches away from re-authentication of a mobile, location-based or otherwise, upon a handoff from one access point to another.

Dependent claims 3, 6, 23, 25, 29, 36, 38, and 43 have been amended to place these claims in their original condition upon filing, and to move some features of these claims to new claims 46-51.

New claims 46-47 are supported, for example, by page 12, line 21, to page 13, line 9.

New claims 48-49 are supported, for example, by page 7, lines 12-16.

New claims 50-51 are supported, for example, by page 10, lines 13-15.

Claim Objections

The objections noted in item no. 2 of the Feb. 2, 2009 Office Action are believed overcome by the amendments to claims 15, 23, 29, and 36.

35 U.S.C. § 103(a) Rejections

Claims 1, 2, 4-6, 9, 10, 12-16, 18, 19, 21, 22, 24, 26, 39-42 and 45 are rejected under 35 U.S.C. §103(a) for obviousness over Stewart (U.S. Patent 6,732,176) in view of Lor (U.S. Patent Application Publication 2004/0068668).

Claims 3, 7, 23, 25 and 43 are rejected under 35 U.S.C. §103(a) for obviousness over Stewart in view of Lor, further in view of Funk (Funk Software, "Comprehensive RADIUS/AAA Solution for the Global Enterprise," Feb. 22, 2003, pages 1-6.

Claims 8, 17 and 44 are rejected under 35 U.S.C. §103(a) for obviousness over Stewart in view of Lor, further in view of Liming (U.S. Patent Application Publication 2002/0055924).

Claims 11, 20, 27-29, 31-35 and 37 are rejected under 35 U.S.C. §103(a) for obviousness over Stewart in view of Lor, further in view of Kwan (U.S. Patent Application Publication 2004/0255154).

Claim 30 is rejected under 35 U.S.C. §103(a) for obviousness over Stewart in view of Lor and Kwan, further in view of Liming.

Claims 36 and 38 are rejected under 35 U.S.C. §103(a) for obviousness over Stewart in view of Lor and Kwan, further in view of Funk.

Independent Claims 1 and 39

As previously mentioned, as amended, independent claim 1 is directed to a mobile client being permitted to roam on the network, and the process that ensues when the mobile client is handed off from one access point to another while roaming. In particular, the amendments, reproduced below, specify that the mobile client is associated with the newly located access point and allowed to continue to access the network but only "upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network":

> "when access is granted, permitting roaming of the mobile client within the network;
>
> during said roaming, when signal quality from a current access point in communication with the mobile client deteriorates sufficiently, locating another access point;

when another access point is located, associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network."

The amendments to independent claim 39, reproduced below, are similar:

"deciding means for deciding whether to grant or deny the ~~user station~~client access to the network based on the authenticity of the identity and the comparison of the location information, and, when access is granted, permitting roaming of the mobile client within the network;

locating means for locating another access point upon detecting, during said roaming, when signal quality from a current access point in communication with the mobile client has deteriorated sufficiently;

second associating means for associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network."

These amendments are directed to overcoming the problem, described in the specification, that occurs when a mobile client, after being authenticated and granted access to a particular network while in a first security zone where the mobile is authorized to access the network, moves to a second security zone of the network, where the mobile is not authorized to access the network. (*See* specification, page 2, line 28, to page 3, line 1). Unless the mobile is re-authenticated at the new location, to determine if the mobile is still authorized to access the network at the new location, the mobile will be allowed to improperly continue to access the network. In effect, the mobile will have evaded the security restrictions of the second zone by gaining access in the first zone, and then moving to the second zone.

However, as the prior art recognizes, another authentication is difficult to perform at that time because it would disrupt any communication session or call the mobile is engaged in at the time of the handoff to the second zone. (*See* Lor, pars. 66, 68, discussed below). In other words, the persistence of an ongoing communication session makes it difficult to re-authenticate the mobile at the new location.

The claimed solution solves this seemingly intractable problem by performing an abbreviated procedure that involves comparing the new location of the mobile with the policy table to determine if the mobile is still authorized to access the network at the new location, without necessarily re-authenticating the identity of the mobile. Due to this abbreviated procedure, any disruption of a communication session that may be in progress is minimal.

The Office Action asserts Lor teaches location based re-authentication of a mobile when it moves to a new location. However, in view of the amendments to claims 1 and 39, Applicant submits the relevant consideration is whether Lor teaches or suggests location based re-authentication of a mobile upon a handoff from one access point to another, and Lor most definitely does not do so.

For example, the following passage from par. 66 plainly teaches against re-authenticating the mobile at the time of the handoff in order to maintain session and application persistency.

> **[0066]** There are two types of persistency requirements for WLAN handoff: session persistency and application persistency. In session persistency, a handoff should not disrupt a session. In other words, the wireless client should not require re-authentication when he travels from one Access Point to another. When the session is transferred from one

(Lor, par. 66).

Similarly, paragraph 68 of Lor teaches that an exchange of session information from the old to the new AP moots the need to re-authenticate the client upon a handoff from one AP to another.

> **[0068]** When a wireless client moves from one zone to another, the client will re-associate with another AP. This re-association leads to the old AP and the new AP exchanging the client session information. Following the framework of 802.11f, or Inter Access-Point Protocol (IAPP), the session information, or connection context, exchanged between the APs may include session information like encryption/decryption key, Service Set, etc. With this exchange, the client at the new location can resume communication immediately, thus eliminating the need of re-authentication.

(Lor, par. 68).

Thus, it can be seen that Lor does not teach or suggest, and in fact teaches away from, "associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network" upon a handoff as required by amended claims 1 and 39. Nor would any system resulting from the obvious combination of Stewart and Lor meet this limitation as such would run contrary to the principle of operation of Lor of avoiding location based re-authentication of the mobile upon a handoff to a new access point. (*See* MPEP §2143.01 (VI) ("If the proposed modification or combination would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.")).

These gaps in teaching of Stewart and Lor are not met by the other cited references, Funk, Liming and Kwan. Accordingly, it is respectfully submitted that amended claims 1 and 39 are allowable.

Independent claims 10 and 27

As previously mentioned, the amendments to independent claim 10 relate to a data structure, accessible by the authentication server, associating identities of clients with their authorized access locations on the network. In particular, the amendments, reproduced below, specify that the authentication server utilizes this data structure to determine whether to grant or deny the client access to the network using the current location information for the client. The amendments also feature a network manager that allows a network administrator to create and update the data structure:

> "a network;
>
> an authenticator for requesting an identity from a client and for associating location information corresponding to the client with the identity; and
>
> a data structure, accessible by an authentication server, associating identities of clients with their authorized access locations;

~~an~~the authentication server, upon receiving the identity and associated location information from the authenticator, ~~for~~ deciding whether to grant or deny the client access to the network ~~based on the identity and the location information~~ by accessing the data structure and determining that the location information corresponding to the client specifies a location that is one of the authorized access locations, if any, for the client as maintained in the data structure; and

a network manager that allows a network administrator to create and update the data structure."

The amendments to independent claim 27, reproduced below, are similar, except that they call for the network manager to be directly connected to the authentication server:

"a data structure, accessible by an authentication server, associating identities of clients with their authorized access locations;

~~an~~the authentication server ~~for~~ deciding whether to grant or deny each of the user stations access to the network ~~based on the corresponding identity and location information~~ by accessing the data structure and determining, for each user station, that the location information corresponding to the user station specifies a location that is one of the authorized access locations, if any, for the user station as maintained in the data structure; and

a network manager, directly connected to the authentication server, that allows a network administrator to create and update the data structure."

Relative to the cited references, Lor does reference a network manager (Lor para. [0115]), but the citation only describes a function to alert a load balance manager when certain statistics reach pre-determined thresholds. Lor also references a central manager (Lor, para. [0104]), but this function relates to the coordination of statistics gathering in a multi-vendor environment. Additionally, Lor discloses a maintenance features managed by a "central management console" with the functions of checking the status of every access points in the managed WLAN..(Lor para. [0102-0103]). However, the maintenance features described do not relate to authentication, e.g.

"broadcast settings, radio frequencies, and device shut-down and bootup times and to provide the ability to distribute AP software upgrades in an automated fashion". (Lor para. [0102]), and

> "manage network access and usage based on user location, manage access to shared network resources such as printers, fax and projectors and collection of advanced Traffic Statistics based on SNMP, RMON and RMON2. (Lor para. [0103])

Further, whereas authentication is an important element of Lor's security methods, as indicated in Lor's description of WLAN security as summarized in Table 1, there is no disclosure in Table 1 of a control function to manage authentication.

Lor is also silent on a data structure, accessible by the authentication server, associating identities of clients with their authorized network access locations.

As for Stewart, Stewart is silent on the topic of network management as well as a data structure, accessible by the authentication server, associating identities of clients with their authorized access location.

Nor does either reference teach or suggest a direct connection between the network manager and authentication server as required by amended claim 27.

Accordingly, neither Stewart nor Lor, considered singly or in combination, discloses a network manager that allows a network administrator to create and access a data structure, accessible by the authentication server, associating identities of clients with their authorized locations, or a direct connection between such network manager and the authentication server.

These gaps in the teachings of Stewart and Lor are not believed met by the other cited references, Liming, Funk, or Kwan.

Accordingly, it is respectfully submitted that amended claims 10 and 27 are allowable.

Dependent claims 2-9, 11-26, 28-38, 40-51

Dependent claims 2-9, 11-26, 28-38, 40-51 are directly or indirectly dependent upon amended claims 1, 10, 27 or 39, and therefore, Applicant respectfully asserts, are allowable at least due to their dependence on an allowable base claim.

Additionally, the Applicant offers the following additional arguments for patentability of dependent claims 46-51.

Dependent claims 46-47

Claim 46 depends from claim 1 and adds the following limitation:

> "wherein the mobile client is associated with the newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network."

Similarly, claim 47 depends from claim 39 and adds the following limitation:

> "wherein the second associating means associates the mobile client with the newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access to the network."

In effect, the additional limitation require location-based re-authentication of the mobile upon a handoff from one access point to another. However, as discussed above, Stewart in view of Lor does not teach, and in fact teaches away from, re-authentication of a mobile upon a handoff from one access point to another, location-based or otherwise, and this gap in teaching is unmet by Liming, Funk or Kwan.

Accordingly, Applicant submits that claims 46-47 are allowable for this additional reason.

Dependent Claims 48-49

Claim 48 depends from claim 8, and adds the following additional limitation:

> "wherein the location information indicates the location of a port of a network switch to which the client is attempting to connect."

Similarly, claim 49 depends from claim 17, and adds the following additional limitation:

> "wherein the location information indicates the location of a port of a network switch to which the client is attempting to connect."

Relative to the cited references, Stewart, Lor and Liming, none teach, suggest, or describe associating location information indicating the location of a particular port to indicate the

physical location of the edge device or wired user station connected to the port, and these gaps in teaching are unmet by Funk or Kwan.

Thus, the Applicant respectfully asserts that claims 47-48 are allowable for this additional reason.

Dependent claims 50-51

Claim 50 depends from claim 24, and recites the following additional limitation:

"wherein the identity includes a smart card identifier."

Similarly, claim 51 depends from claim 37, and recites the following additional limitation:

"wherein the station identities includes a smart card identifier."

Applicant respectfully submits that these limitations are neither taught nor suggested by the cited references, considered singly or in combination, and accordingly that claims 50-51 are allowable.

CONCLUSION

For all the foregoing reasons, claims 1-51 are allowable, and the Examiner is earnestly solicited to pass this application to issuance. If there are any questions, the Examiner is urged to call the undersigned at (949) 759-5269.

Respectfully submitted,

Date: July 28, 2009

/Robert C. Laurenson/
Robert C. Laurenson
Reg No. 34,206

HOWREY LLP
2941 Fairview Park Drive, Box 7
Falls Church, VA 22042
Tel: (650) 798-3548
Fax: (650) 798-3600